

## A10 Control

以統一的管理、控制及分析平台實現敏捷作業及自動化

這款集中管理及分析平台可協助您完整控制 A10 解決方案，不論部署於內部、雲端或混合環境都沒問題。

### 敏捷管理及智慧型分析

現代網路及安全基礎架構日漸複雜，再加上各界快速採用 AI 及雲端技術，讓組織在管理及支援關鍵任務服務和業務時面對重大挑戰。

部署地點一旦橫跨各個不同地區及多個雲端環境，瞭解網路基礎架構資源及追蹤服務狀態就會複雜又耗時。精準的容量規劃及立即回應擴充需求，對 AI 應用程式及應用程式服務基礎架構而言至關重要，因為這類基礎架構不但需要更高的流量及交易量，也非常容易受到延遲影響。因此管理員應運用敏捷管理及智慧型分析功能，建立高效的作業及管理工作流程。

A10 Control 是新一代的管理及分析平台，適用於 A10 解決方案，可整合現有的 A10 Harmony 控制器及 aGalaxy 功能。A10 Control 可集中管理 A10 安全和基礎架構解決方案，包括部署在任何網路或雲端環境的 ADC、DNS 及 DDoS 防護。集中平台可協助收集、分析和報告通過 A10 設備的應用程式及服務流量，並透過智慧型分析功提供可視化的資訊，幫助掌握服務和安全態勢。

平台



虛擬設備

相關的  
產品與服務



ADC



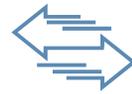
A10 Defend  
DDoS 防護

## 優勢



### 獲得 即時智慧分析及觀察能力

組織必須保證服務可持續運作。因此營運團隊的關鍵任務，就是瞭解服務狀況並具備觀察能力。A10 Control 可對採用 A10 先進核心作業系統 (ACOS) 的 A10 裝置，收集通過其中流量的相關指標資料和交易記錄，並提供深度可視性，協助掌握服務及網路基礎架構的情況。智慧型分析及可自訂警示有助於識別潛在問題，避免影響最終使用者，並可存取情境式流量資料和記錄，主動進行疑難排解。



### 提升 營運效率

組織可簡化工作流程及實現自動化流程，以提升營運團隊的敏捷度和效率。裝置生命週期管理包含備份、健全狀態檢查、軟體升級、庫存及授權管理，可說是困難又耗時的作業。A10 Control 的智慧型自動化功能和各項工具能夠促進高效作業，幫助管理部署在資料中心乃至於任何雲端等各種基礎架構的大量設備和服務。

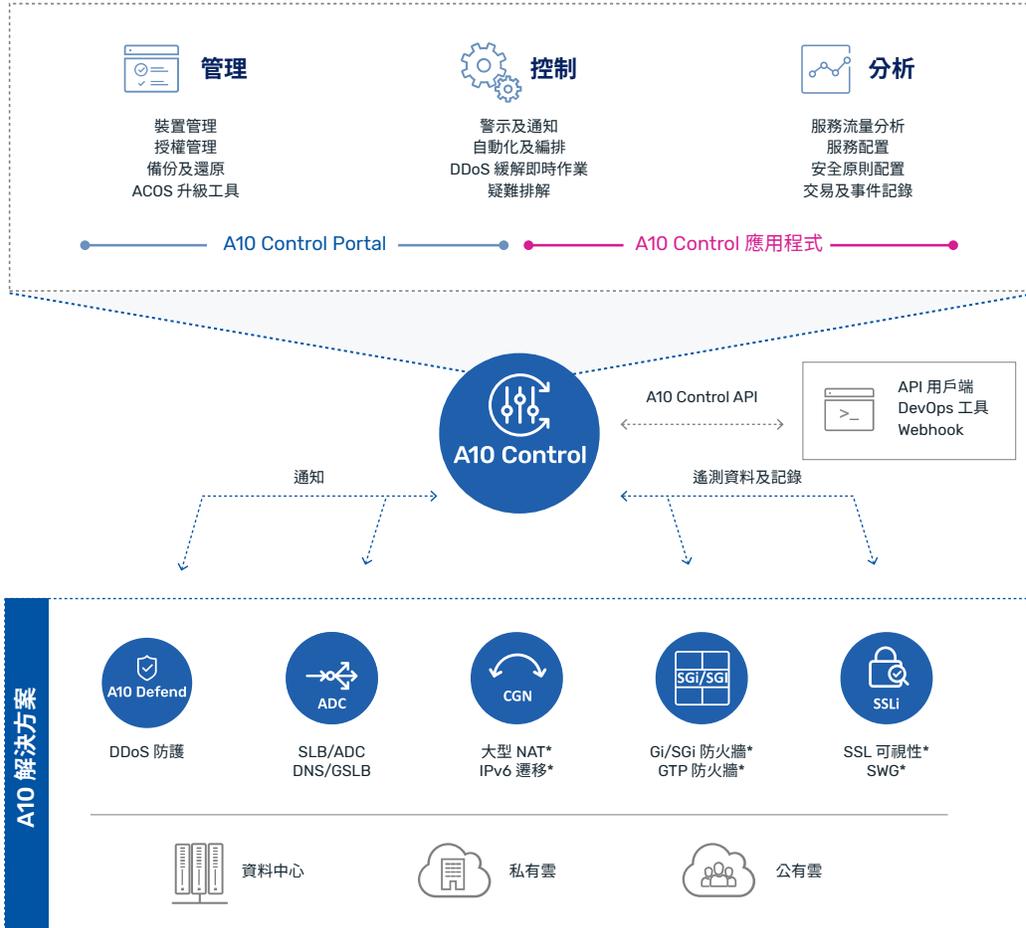
全方位 API 能夠輕鬆整合熱門的 DevOps、基礎架構即程式碼和觀察能力工具鏈，以及主要的公有雲和私有雲基礎架構。



### 簡化 管理服務及安全性

單一管理平台適用於任何 A10 解決方案；A10 獨一無二的技術優勢之一，就是所有 A10 解決方案均於共同 OS (ACOS) 執行，不受平台或外型尺寸影響。現在 A10 Control 成為管理員需要的唯一管理平台，整合了 A10 Harmony 控制器及 aGalaxy 的各項功能。

A10 Control 以 AI 支援的效能管理功能準確事先預測問題，可協助簡化 IT 作業並改善服務連續運作時間。



\* A10 Control 應用程式將於 2025 年推出

圖 1：A10 Control 是集中的管理及作業平台，適用於 A10 基礎架構服務和安全解決方案。

# 特色

## 集中管理



### 裝置生命週期管理

集中的裝置生命週期管理功能，適用於 A10 硬體及虛擬設備，包括公有雲、私有雲及裸機。直覺操作的庫存和授權管理功能，適用於多種 A10 Thunder 及 A10 Defend DDoS 設備。自動化例行作業，例如備份、庫存報告，以及排程自動化軟體升級。



### 裝置分析

A10 裝置可跨不同地理區域部署在各種網路及雲端環境中，提供詳細的裝置層級分析功能。裝置健全狀態監控及儀表板可提供系統資源使用率、裝置位置、流量及連線指標、交易記錄和事件資訊。



### 警示和報告

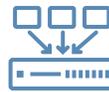
從 A10 裝置收集的指標和記錄會依據使用者定義規則建立關聯及評估，以便針對異常事件提出警示。這類警示可透過電子郵件通知及 / 或 Webhook 傳送，並使用 Slack 及 Microsoft Teams 等協作工具實現自動化行動。

## 服務作業



### 服務及原則管理

利用共用資源從中央主控台為部署在不同地區的 A10 裝置變更配置及執行安全原則更新，例如類別清單或 IP 清單。



### 多租戶

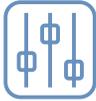
彈性的多租戶架構和角色型存取控制功能，可讓各個應用程式團隊及服務負責人擁有名為組織單位 (organization-unit) 的租戶工作空間，以便管理各自的服務與作業。租戶分配可彈性地在租戶中設置多個 A10 裝置叢集，或是精細地為 A10 裝置的各個 L3V/ADP 分區指派租戶。



### API 驅動的自動化與整合

全方位的 A10 Control API 可利用 Ansible、Chef 及 Jenkins 等 DevOps 工具鏈輕鬆整合，透過 A10 Control 自動化 A10 裝置配置管理，並為受管理的 A10 解決方案簡化監控及作業工作流程。

## 架構及系統



### 可靠的控制器平台

A10 Control 以穩固的 RHEL 基礎建構而成搭配使用 Kubernetes 的微架構，除了可讓控制器達到最高可用度，也能確保完整的法規遵循，符合最新的業界標準。控制器能以安全方式收集和處理 A10 裝置的各種遙測資料，絕對不會處理通過 A10 裝置資料平台的服務流量。這項架構也能在控制器與 A10 裝置之間連線中斷時，確保絕對不會發生服務流量中斷的情況。



### 提升安全性及維護能力

包含 Harmony 控制器在內的 A10 產品系列，多年來持續使用微服務架構。A10 Control 設計使用最新及最出色的 RHEL 軟體，並採用新一代架構。這有助於提升系統的安全性及維護能力，特別是在安全性及 CVE 修補程式方面。



### 部署選項

控制器可安裝為自助管理軟體解決方案，在客戶環境中以單節點或多節點高可用性 (HA) 部署。在 HA 部署中，微服務及控制器的資料儲存會分散在節點之間。

如需深入瞭解系統需求及安裝 A10 Control 的先決條件，請參閱最新產品文件或聯絡 A10 銷售代表。



### 翻新架構提升穩定度及效能

A10 Control 用於建構產品的所有元件、框架和技術均為升級版，大幅提升穩定度及效能。A10 Control 使用的資料庫系統有別於 Harmony 控制器，提供簡化及低延遲的資料作業，此外還以全新的標準型技術提供使用者驗證管理。

# A10 Control 應用程式

以解決方案為基礎的全方位分析、配置及服務作業工具，全部都內建為 A10 Control 的應用程式。視管理的授權及服務類型而定，會解鎖適當的應用程式，並在選定的租戶之下啟動提供服務。



## 應用程式交付控制器 (ADC) 應用程式

ADC 應用程式提供 ADC 配置工具用於管理單站台或多站台部署，此外也提供全方位見解，協助掌握應用程式流量及趨勢、延遲深入研究及分析，以及 ADC 及應用程式伺服器健全狀態等更多項目。其中結合豐富的分析功能和情境式記錄，有助於偵測異常趨勢並簡化疑難排解。

執行 DNS 服務時，ADC 應用程式會自動顯示以 DNS 為主的分析資訊。



## A10 Defend Orchestrator (ADO) 應用程式

DDoS 防護管理 (前身為 aGalaxy) 目前以 ADO 應用程式在 A10 Control 提供使用。其中提供直覺操作的 DDoS 防護配置功能，適用於 A10 Defend DDoS Detector 及 Mitigator，此外還有監控區域的即時流量圖表、編排防護工作流程乃至於即時緩解主控台等功能，幫助在發生 DDoS 事件時加以因應。

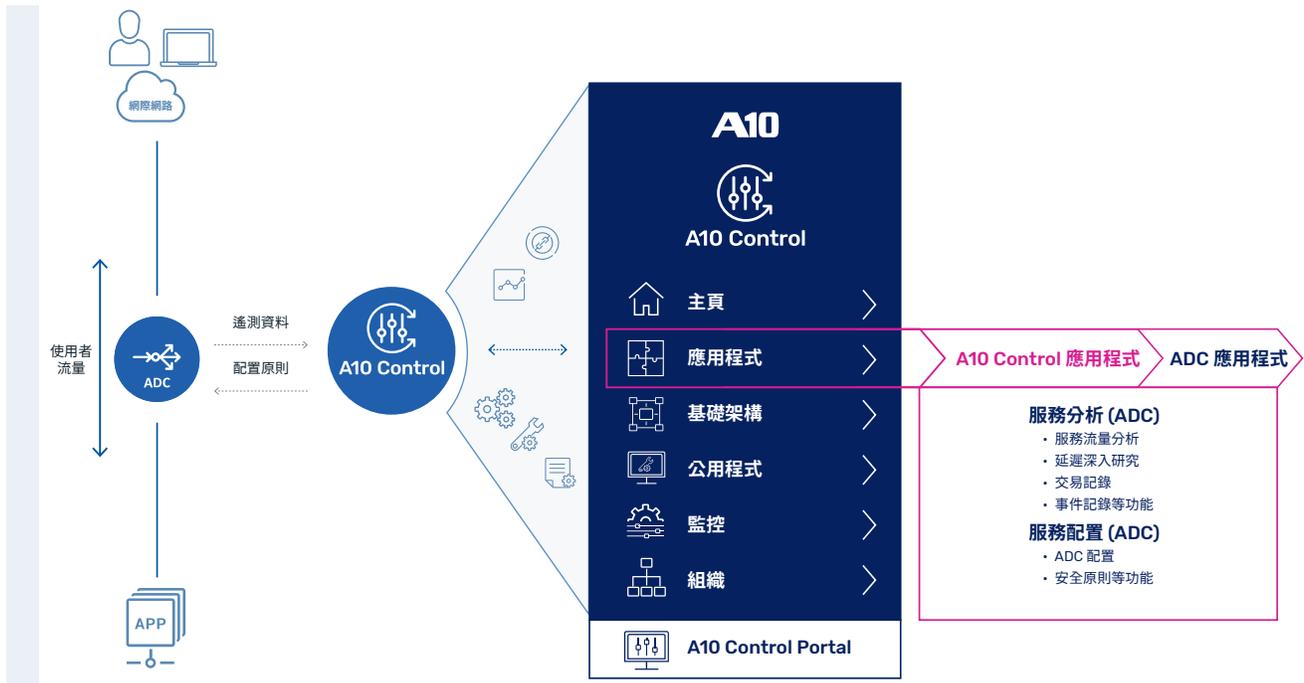


圖 2：A10 Control 透過控制平台收集 A10 裝置的遙測資料，並利用服務專屬的 A10 Control 應用程式提供分析及控制功能。

# 使用案例

## 支援的 A10 解決方案

### 應用程式交付

高效能的進階負載平衡解決方案，讓應用程式高度可用、加速且安全無虞。部署搭配 A10 Thunder ADC 或 Thunder CFW-ADC，可採用任何外型尺寸，包括硬體、Hypervisor 型軟體、裸機、容器，或是混合雲及多雲環境。

### DNS

可擴展且安全無虞的 DNS 負載平衡及快取解決方案，讓 DNS 基礎架構更具韌性且效率更高。部署搭配 A10 Thunder ADC 或 Thunder CFW-ADC，可採用任何外型尺寸及環境。

### DDoS 防護

全方位的 DDoS 防禦解決方案，具備可擴展、經濟實惠、精準及智慧化等特色，協助組織確保延長服務連續運作時間。部署搭配 A10 Defend DDoS Detector 及 Mitigator。

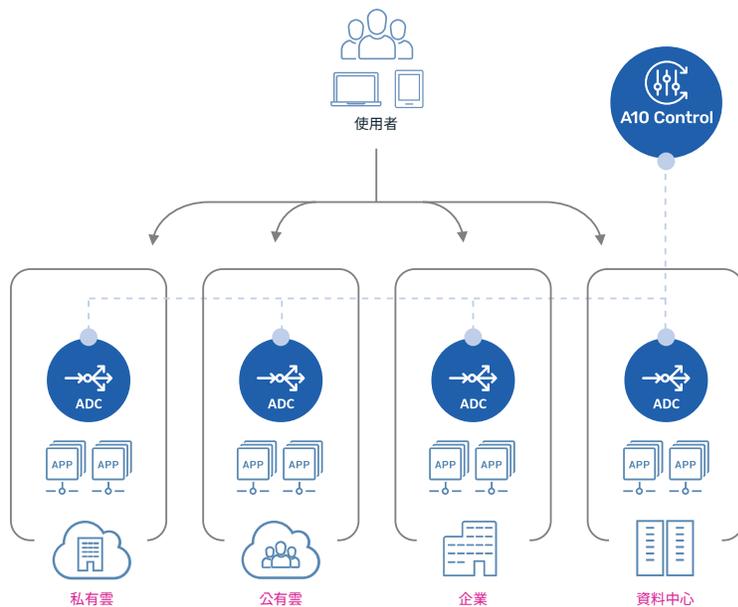


圖 3：多雲 ADC 使用案例。

### 多雲應用程式交付部署

A10 Control 可集中管理及控制部署在混合雲或多雲環境的應用程式交付服務，並提供以下功能：

- ADC 分析
- ADC 及安全原則執行
- ADC 裝置和配置管理等功能

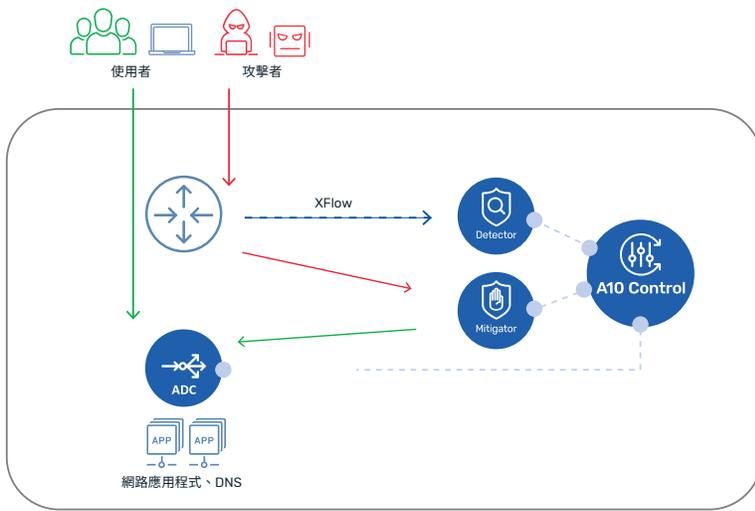


圖 4：DDoS 防護使用案例。

## 適用於網路應用程式及 DNS 的 DDoS 防護

A10 Defend DDoS Orchestrator (ADO) 於 A10 Control 執行運作，搭配使用 Mitigator 及 Detector，可實現智慧自動化防護功能，對抗鎖定應用程式服務及 / 或網路基礎架構的現代 DDoS 攻擊。

ADO 應用程式提供以下功能：

- DDoS 防禦編排及自動化
- DDoS 緩解控制台
- DDoS 防禦原則配置
- 事件報告等功能

如果 A10 ADC 用於應用程式服務，也可由相同的 A10 Control 進行管理和控制。

# 詳細功能清單

## A10 Control Portal

裝置管理	
庫存清單	以多種形式顯示完整的裝置庫存，例如個別裝置檢視及叢集檢視 (單節點、VRRP-a 配對等)，提供一般系統資訊。
裝置管理及分析	為 A10 裝置提供詳細的叢集和裝置層及分析功能，包括系統及網路資訊，並可分析系統資源使用情形及流量統計資料。
裝置備份及還原	A10 裝置配置可定期備份，儲存於 A10 Control 之中。備份可在需要時用於還原裝置。
ACOS 映像升級	映像升級公用程式提供直覺可靠的 ACOS 映像升級流程，包含手動及排程方法，適用於註冊的 A10 裝置。所有升級作業記錄均於歷史記錄檢視中提供。
監控及警示	
服務層級健全狀態監控及警示	自訂觸發規則可使用各種服務層級指標和閾值，用於監控服務流量及狀況。警示可透過電子郵件及 Webhook 傳送，更輕鬆與現有監控系統整合。
裝置層級健全狀態監控及警示	精細的裝置層級觸發規則可依據各種項目設定，包括基礎架構 / 裝置資源使用情況、基於裝置層級流量的閾值，以及系統記錄。警示可透過電子郵件及 Webhook 傳送，更輕鬆與現有監控系統整合。
報告	提供租戶層級庫存報告及每項服務的作業報告，並可針對特定期間進行排程。報告可下載為 PDF 格式，或透過電子郵件及 Webhook/HTTP POST 傳送。
事件和稽核記錄	事件檢視器可從所有註冊的 A10 裝置中，提供整合的系統及服務事件記錄。稽核檢視器可存取 A10 控制器的稽核記錄，以及所有註冊的 Thunder 和授權管理活動記錄。提供精細的記錄篩選條件，記錄可下載為 CVS 格式。
管理及公用程式	
多租戶管理	多租戶功能提供精細的角色型存取，適用於應用程式團隊及服務負責人。每個租戶 (組織單位) 可與 A10 裝置分區 (ADP/L3V) 層級對應。
CLI 命令公用程式	單一或批次 CLI 命令可同時於多個裝置分區遠端執行。
共用配置資源集區	類別清單、封鎖 / 允許清單、SLB 範本、安全範本及 TLS/SSL 憑證等共同配置資源 / 範本，可建立為共用資源，並在任何註冊的 A10 裝置之間使用，不受服務類型影響。
授權管理	A10 Control 以企業授權管理工具的形式運作，可用於管理及控制註冊 A10 裝置的 FlexPool 容量授權。
使用者管理	角色型存取控制提供彈性的使用者管理功能。例如，存取區域可依據組織、租戶、裝置或特定服務 / 分區進行設定，而權限層級可以是管理員、作業人員，或特定作業的自訂規則。
驗證管理	除了本機驗證以外，也可選擇 Azure、Okta 或 LDAP 等身分供應商 (IdP) 進行外部驗證和單一登入 (SSO)。

# A10 Control 應用程式

## 應用程式交付

### ADC 分析 (每項虛擬服務)

- 即時 ADC 服務層級 KPI，包含流量資訊、錯誤率及延遲
- 基於使用者流量的分析，包括使用者見解 (位置、瀏覽器)、前 k 個資訊、請求見解、時間序列延遲等項目
- 基於地理位置的流量分析，協助掌握延遲及流量
- 常見通訊協定的 ADC 服務分析 (HTTP/S、SSL 及 HTTP2)
- ADC 叢集分析，提供資源使用見解
- 應用程式服務分析，提供詳細的應用程式服務狀況及趨勢
- 應用程式伺服器分析，協助掌握伺服器健全狀況及狀態
- 延遲深入研究及分析，協助掌握端對端延遲狀況，涵蓋從請求到回應的完整週期

ADC 交易記錄檢視器，提供用戶端、請求及回應資料和延遲資訊

事件及警示記錄檢視器

集中 ADC 配置工具

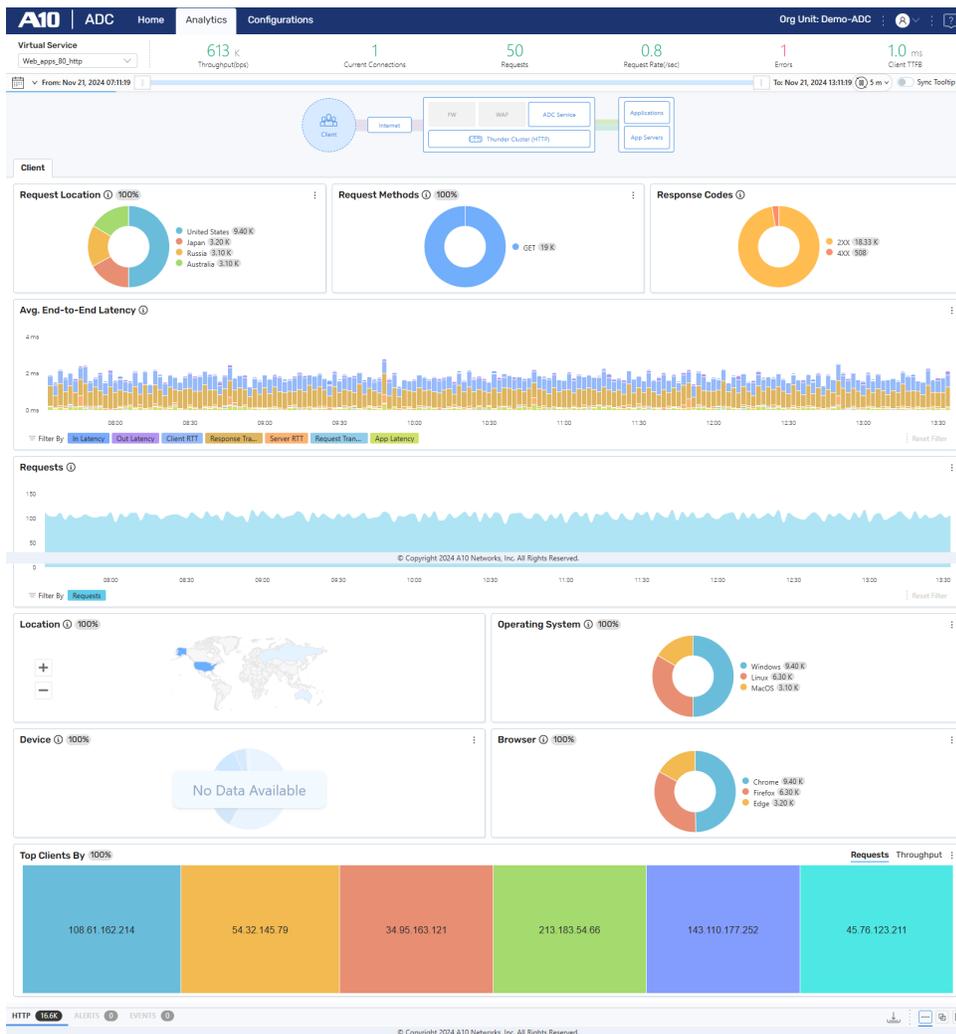


圖 5：ADC 應用程式：ADC 分析提供基於用戶端的見解。

## Defend Orchestrator

ADC 交易記錄檢視器，提供用戶端、請求及回應資料和延遲資訊

- DDoS 防護工作流程編排
- 在 Detector 與 Mitigator 之間實現緊密順暢的通訊
  - 控制及轉送 DDoS 訊號提供自動化的防禦作業
  - 傳送流量轉移通知，以便在反應式部署中進行清理
  - 手動或自動化的遷移行動
  - 攻擊結束後自動提出 DDoS 事件報告

概要儀表板協助掌握 DDoS 事件及活動

受監控區域的即時流量圖表和統計資料

DDoS 緩解控制台提供即時防禦作業和監控

為 DDoS 事件、受保護區域及裝置庫存等提供隨需及排程報告

隨需或自動化的封包擷取工具

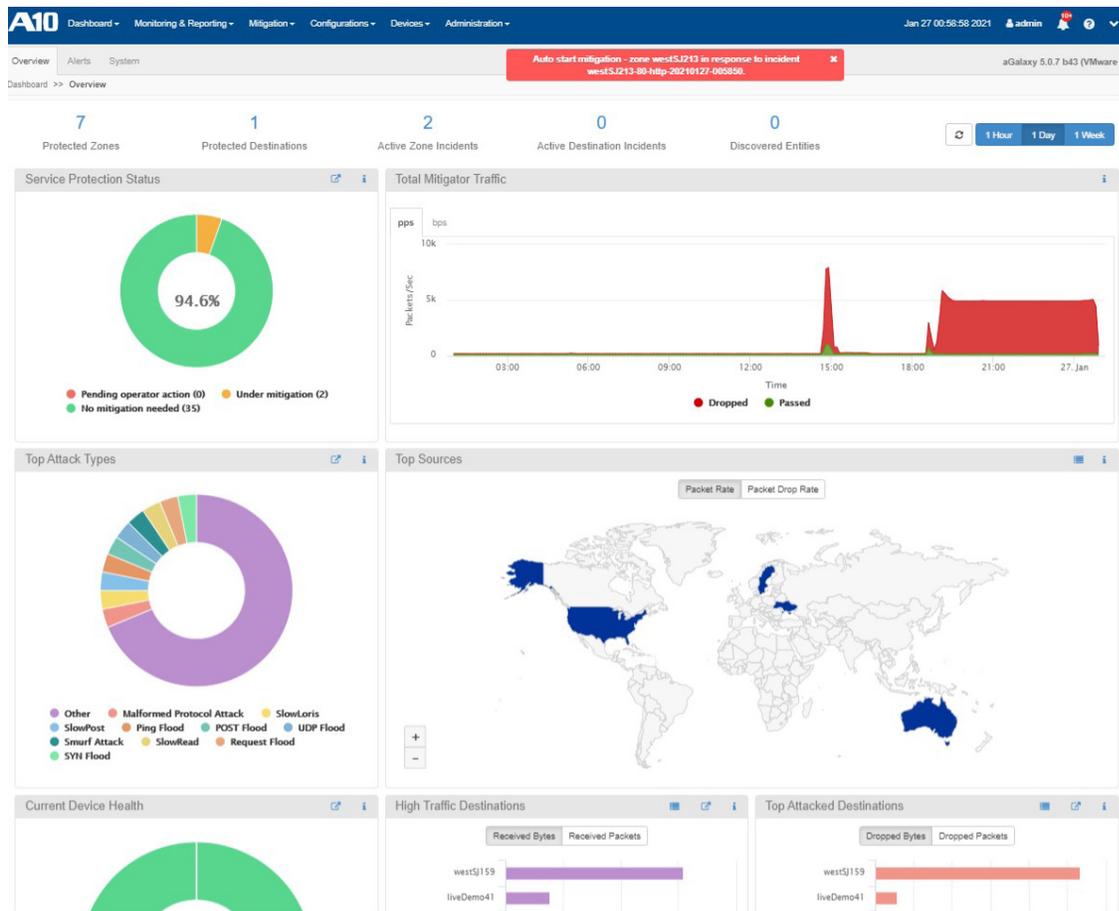


圖 6：A10 Defend Orchestrator 儀表板提供即時攻擊統計資料及 DDoS 事件摘要。

## 深入瞭解

關於 A10 Networks

聯絡我們

APAC@a10networks.com

©2025 A10 Networks, Inc. 保留所有權利。A10 Networks、A10 Networks 標誌、ACOS、Thunder、Harmony 和 SSL Insight 是 A10 Networks, Inc. 在美國和其他國家/地區的商標或註冊商標。所有其他商標均為其各自所有者的財產。A10 Networks 對本文件中的任何不精確處不承擔任何責任。A10 Networks 保留變更、修改、轉讓或以其他方式修訂本出版品的權利，恕不另行通知。有關商標的完整清單，請造訪：[A10Networks.com/a10trademarks](https://www.a10networks.com/a10trademarks)。

Part Number: A10-DS-15139-TW-01 Jan 2025

